REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
AUG 2011	Conference Paper (Post Print)	OCT 2009 – NOV 2011

4. TITLE AND SUBTITLE

USING FUNCTIONAL PROGRAMMING AND ACCESS-CONTROL LOGIC FOR MISSION ASSURANCE

5a. CONTRACT NUMBER In-House IMPDSNIH

5b. GRANT NUMBER N/A

5c. PROGRAM ELEMENT NUMBER 61102F

6. AUTHOR(S)

AFRL:
Thomas Vestal, Sarah Muccio

Syracuse University:
Susan Older, Shiu-Kai Chin

5d. PROJECT NUMBER IMPD

5e. TASK NUMBER SN

5f. WORK UNIT NUMBER IH

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RIGA
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TP-2012-006

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved For Public Release; Distribution Unlimited. PA #: 88ABW-2011-4283
Date Cleared: 8 AUG 2011

13. SUPPLEMENTARY NOTES
Publication presented at 23rd Symposium on Implementation and Application of Functional Languages, 3-5 Oct 2011, Cambridge University, UK. One or more of the authors is a U.S. Government employee working within the scope of their Government job; therefore, the U.S. Government is joint owner of the work and has the right to copy, distribute, and use the work. All other rights are reserved by the copyright owner.

14. ABSTRACT

Critical missions require the guarantees provided through formal verification and functional programming. This provides a strong basis for decisions that must be assured in a contested cyber environment. We present a framework for educating future cyber leaders on these im0portant concepts and tools.

15. SUBJECT TERMS
Impregnable design, trustworthy computer components, tools for trustworthiness, methods for verification, FPGA instructions

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	19b. TELEPHONE NUMBER (*Include area code*)
U	U	U	UU	3	ANNA WEEKS	N/A

Using Functional Programming and Access-Control Logic for Mission Assurance

Thomas N.J. Vestal[1], Sarah L. Muccio[1], Susan Older[2] and Shiu-Kai Chin[2]

[1]Air Force Research Laboratory, Information Directorate, Rome, New York 13441, USA
[2]EECS Department, Syracuse University, Syracuse, New York 13244, USA

Abstract – **Critical missions require the guarantees provided through formal verification and functional programming. This provides a strong basis for decisions that must be assured in a contested cyber environment. We present a framework for educating future cyber leaders on these important concepts and tools.**

Index Terms – Functional programming, formal verification, education, mission assurance

THE PROBLEM

The U.S. Department of Defense (DoD) depends increasingly on technology and cyberspace to execute critical missions. Recent congressional and White House reports, [1][2] concurred on the need to assure these missions especially in a contested cyber environment – an environment that may be under attack.

The DoD requires employees that can assess the quality of the specification, design and implementation of a mission including all supporting technology. This requires educating personnel on verification methods including formal mathematics, access-control logic [3] and the science of mission assurance [4].

APPROACH

Functional languages such as Haskell [5] and ML [6] are well suited for (1) animating specifications, (2) prototyping implementations, and (3) formal verification. Formal verification and reasoning about access-control decisions and security policies are important for assuring critical DoD missions. Design specifications and implementations can be animated using functional languages to validate specifications and requirements. Theorem provers such as HOL [7] can then be used to verify correctness and properties of implementations. Tools such as HOL enable independent verification by third parties, which is the key to mission assurance. The DoD must be able to establish that vendors have correctly implemented mission critical systems. Functional languages and theorem provers such as Haskell and HOL enable DoD employees to independently verify and assure that systems meet mission requirements.

Approved for Public Release; Distribution Unlimited: 88ABW-2011-4283
Dated 8 Aug 2011.

We have used access-control logic and HOL to specify and verify DoD concepts of operations [8]. This work involves trust establishment and preserving integrity of command and control of Air Force systems.

Our hypothesis is that formal math and logic in the form of Haskell and HOL help engineers create and verify systems in ways that make it easier to credibly document and assess claims of correctness and security. As Professor David Parnas champions, we must demand "disciplined, careful, complete work" [9].

METHOD

To meet DoD assurance needs, we are experimenting with a methodology to educate future DoD employees and contractors on the science of mission assurance through the use of functional programming, access-control logic, and formal verification using theorem proving. We view these as essential capabilities for accurately describing, prototyping, and verifying systems for critical missions.

Since 2003, we have educated undergraduate and graduate students as well as practicing engineers in practical uses of access-control logic [10][11][12]. This has allowed us to develop this comprehensive educational framework to teach concepts of formal verification for mission assurance.

In 2011, the Air Force Research Laboratory Information Directorate created the Information Assurance Internship [13] – a follow-up to the Advanced Course in Engineering (ACE) Cyber Security Boot Camp [14][15]. We implemented this methodology during the internship which was to undergraduates and newly graduated students. We used several Air Force missions as use cases for the access-control logic to formally verify mission assurance.

INFORMATION ASSURANCE INTERNSHIP

During the 2011 Information Assurance Internship, undergraduate students were challenged to learn a functional programming language in two, four hour long sessions. They were taught Haskell first then HOL. They incorporated the Haskell programs into the design of their weekly projects.

Their projects focused on designing secure systems for mission specific tasks.

These students used Haskell to animate the specifications of their engineering design. They demonstrated their working code during their presentations in which they highlighted the specialized language syntax and semantics.

The students also incorporated the HOL theorem prover into their later projects. This allowed for a formal verification of their systems. It also created a common reference for the teams of students to debate the merits of their designs. These foundational skills provide the students with tangible take-a-ways for future research and design.

Conclusion and Future Work

Overall the results of our work show promise that not only practicing engineers can learn how to verify a mission, but undergraduate students as well. With a relatively small amount of course work, our students have been able to reason about access-control, security and mission assurance. This allows the students to precisely describe problems in a specification, reason about the security concerns and formally verify the implementation of a design.

This upcoming semester Syracuse University and the Air Force Research Laboratory partnered to produce 18-credits of a Cyber Engineering Curriculum. This takes the normal junior year computer engineering curriculum and adds a security focus to each course – examples include secure operating systems, secure computer architecture and secure hardware design laboratory. In the future, we plan to expand this curriculum to include a full minor in the security field.

Acknowledgments

The authors would like to acknowledge the Air Force Office of Scientific Research for their sponsorship and support of these scientific endeavors. The authors would also like to acknowledge the support of Ms. Sonja Glumich and Mr. Brian Kropa of the Air Force Research Laboratory for their support in the implementation of these teaching methods during the Information Assurance Internship Program.

Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the U.S. Air Force Research Laboratory, United States Air Force, Department of Defense, or the United States Government.

References

[1] "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Security (CSIS), December 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

[2] White House, "Cyberspace Policy Review," May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[3] S-K. Chin and S. Older, *Access Control, Security, and Trust: A Logical Approach*, CRC Press, 2011.

[4] K. Jabbour and S. Muccio, "The Science of Mission Assurance," Journal of Strategic Studies, v4 issue 2, 2011, pp. 61-74.

[5] The Haskell Programming Language. http://www.haskell.org

[6] L. C Paulson, *ML for the Working Programmer*. Cambridge University Press, July 1996.

[7] M.J.C. Gordon and T.F. Melham, *Introduction to HOL: A Theorem Proving Environment for Higher Order Logic*, Cambridge University Press, New York, 1993.

[8] S-K. Chin, S. Muccio, S. Older, and T. Vestal, "Policy-Based Design and Verification for Mission Assurance," in Igor Kotenko and Victor Skormin (Eds.), Computer Network Security, 5th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2010, St. Petersburg, Russia, September 2010.

[9] D. Parnas, "The Risks of Stopping too soon," Commun. ACM 54(6): 31-33 (2011)

[10] S-K. Chin, "Educating Engineers to Design Trustworthy Systems," Indo-US Conference and Workshop on Cyber Security, Cyber Crime, and Cyber Forensics, August 19-21, 2009, Kochi, India. http://www.ecs.syr.edu/faculty/chin/papers/secureHW.pdf

[11] S-K Chin and S. Older, "A Logical Approach to Access Control," Security, and Trust, Indo-US Conference and Workshop on Cyber Security, Cyber Crime, and Cyber Forensics, August 19-21, 2009, Kochi, India. http://www.ecs.syr.edu/faculty/chin/papers/acl.pdf

[12] S-K Chin. "Logic Design for Access Control, Security, Trust and Assurance," Engineering of Reconfigurable Systems and Algorithms (ERSA'11), July 25-26, 2011, Las Vegas, Navada.

[13] Information Assurance Internship. Air Force Research Laboratory - Information Directorate, http://www.wpafb.af.mil/shared/media/document/AFD-101001-007.pdf

[14] D. Carnevale, "Basic training for anti-hackers: An intensive summer program drills students on cybersecurity skills," The Chronicle of Higher Education, September 23 2005.

[15] K. Jabbour and S. Older, "The advanced course in engineering on cyber security: A learning community for developing cyber-security leaders," in Proceedings of the Sixth Workshop on Education in Computer Security, July 2004.

Author Information

Shiu-Kai Chin is a Professor in the Department of Electrical Engineering and Computer Science at Syracuse University. He is also Co-Director of the Center for Information and Systems Assurance and Trust (CISAT).

Sarah L. Muccio is a Mathematician in the Cyber Science branch of the Air Force Research Laboratory's Information Directorate. She received her Ph.D in Applied Mathematics from North Carolina State University in 2007.

Susan Older is an Associate Professor in the Department of Electrical Engineering and Computer Science at Syracuse University.

Thomas N.J. Vestal is a Computer Engineer in the Cyber Science branch of the Air Force Research Laboratory's Information Directorate. He is a Computer Engineering Ph.D candidate at Syracuse University.